UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,928	08/09/2001	Rodric C. Fan	TRMB-2096	6041

70409 7590 09/16/2009

TRIMBLE NAVIGATION LIMITED C/O WAGNER BLECHER
123 WESTRIDGE DRIVE
WATSONVILLE, CA 95076

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
09/16/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/927,928	FAN ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6,8-11,15-17,20,25-27 and 29-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-4,6,8-11,15-17,20,25-27 and 29-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07.09.09*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to Applicant's Remarks and Amendments filed June 4, 2009.

Claims 5, 7, 12-14, 18-19, 21-24, and 28 remain cancelled.

Claims 1, 6, 10, and 29 are amended.

Claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 are pending and herein considered.

Response to Arguments

Applicant's arguments in response to the Examiner's 35 USC 103(a) rejection of claims 1-4, 6, 8-11, 15-17, 20, 25-27 and 29-35 have been fully considered but they are not persuasive.

In response to Applicant's arguments regarding Kaufman's alleged failure to teach or suggest "transmitting the encrypted first key separate from the encrypted data packet" in claim 1, the Examiner respectfully disagrees. Applicant once again points to col.3 lines 21-35 of Kaufman which, according to Applicant, "teaches away" from Applicant's claims by "requiring the key and the payload always be included together in the same message rather than being sent separately." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e. wherein the second

transmission cannot include the encrypted first key) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Although it may be Applicant's intention to claim an invention wherein no transmission but the first would include the encrypted first key, Applicant's claims fail to claim any such intention. Instead, Applicant's claims call for the transmission of Applicant's first encrypted key in a first transmission separate from the encrypted data packet and the subsequent transmission of the encrypted data packet in a second transmission without specifying that the second data packet not include the first encrypted key. The Examiner once again draws attention to column 3, namely likes 21-25 wherein Kaufmann clearly provides for "in the course of session establishment, each node tells the other what its encrypted version of the shared key is and to use this in any data packets communicated between them." The Examiner has treated this transmission of the encrypted key as Applicant's "transmitting the encrypted first key separate from the encrypted data packet… in a first transmission" As such, the Examiner maintains her belief that the secondary transmissions of encrypted data packets within Kaufmann, whether or not those transmissions include the encrypted first key, teach Applicant's "transmitting the encrypted data packet over a wireless link to a gateway in a second transmission" insofar as they include the encrypted data packet and insofar as Applicant has not restricted this transmission to the encrypted data packet alone. Applicant's use of an open-ended transitional phrase within his claims, namely "comprising," allows the Examiner to apply prior art which encompasses each of

the elements or limitations therein as well as additional, unnamed elements or limitations. If it is Applicant's intention to claim an invention wherein the encrypted key cannot or will not be transmitted outside of the first transmission, it is imperative that he claim it as such.

Applicant's arguments concerning claims 6, 10, and 29 rely upon those given above with regards to claim 1. These arguments are equally unpersuasive.

Applicant's arguments concerning the remaining claims are based upon their dependency upon the independent claims discussed above. These arguments are equally unpersuasive.

It is based upon the above made arguments in view of the references in their entirety that the Examiner maintains her 35 USC 103(a) rejection of claims 1-4, 6, 8-11, 16-17, 20, 26, 27 and 29-35, included below in an amended form to reflect Applicant's amendments.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-4, 6, 9-11, 16-17, 20, 26-27, 29-33 and 35 remain rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent No. 5,081,678 to *Kaufman et al.*, and further in view of United States Patent Application Publication No. 2002/0004898 A1 to *Droge*.

As per **claim 1**, Kaufman teaches a method for transmitting secured data over a wireless link, the method comprising:

utilizing a first key to encrypt a payload (col.3 lines 6-13);

adding a header to the encrypted payload to form a data packet (col.4 lines 59-68);

utilizing a second key to encrypt the first key (col.3 lines 14-20);

transmitting the encrypted first key separate from the encrypted data packet to a wireline device in a first transmission from a wireless device, wherein the wireline device decrypts the encrypted first key (col.3 lines 14-25); and

transmitting the encrypted data packet over a wireless link to a gateway in a second transmission from the wireless device, decrypting the encrypted data packet to recreate the encrypted payload and the header, and forwards the encrypted payload and the header to the wireline device over an open network (col.3 lines 5-35, 51-62);

and utilizing the wireline device and the first key from the first transmission to decrypt the encrypted payload (col.3 lines 51-62)

Kaufman fails to specifically disclose utilizing a third key to encrypt the data packet and decrypting the encrypted data packet at gateway.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second key to provide for heightened security for the information provided in the data packet.

As per **claim 2**, the combined method of Kaufman and Droge wherein the first key comprises a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 3**, the combined method of Kaufman and Droge teaches transmitting the encrypted first key to the wireline device, wherein the wireline device decrypts the encrypted first key using a private key associated with the second key (Droge par.66; Kaufman col.3 lines 27-31).

As per **claim 4**, the combined method of Kaufman and Droge teaches wherein the third key comprises a symmetric session key (Kaufman col.3 lines 6-20).

As per **claim 6**, Kaufman teaches a device for transmitting secured data over a wireless link, the device comprising:

an encryption engine which generates a first key (col.3 lines 6-13), encrypts a payload according to the first key (col.3 lines 6-13), adds a header to the encrypted payload to form a data packet (col.4 lines 59-68), encrypts the first key according to a second key (col.3 lines 14-25); and

a wireless transceiver coupled to the encryption engine, the wireless transceiver transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from the device (col.3 lines 14-20) and transmitting the encrypted data packet over the wireless link to a gateway in a second transmission from the device which decrypts the encrypted data packet (col.3 lines 21-33) to recreate the encrypted payload and the header (col.3 lines 21-33), and forwards the encrypted payload and the header to the server over an open network (col.3 lines 21-33);

wherein the server decrypts the encrypted first key received in the first transmission and decrypts the encrypted payload of the second transmission using the decrypted first key (col.3 lines 27-31).

Kaufman fails to specifically disclose encrypting the data packet according to a second key and decrypting the encrypted data packet at the gateway. Kaufman also fails to specifically disclose a wireless link to the gateway.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge

Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireline and wireless networks and links that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second session key to provide for heightened security for the information provided in the data packet as well as the wireless networks and links as described in Droge to provide for increased network flexibility.

As per **claim 9**, the combined method of Kaufman and Droge teaches wherein the first key employs a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 10**, Kaufman teaches a method for secured communication between a mobile device and a server on a wide area network, the method comprising:

encrypting a payload at the device using a first session key (col.3 lines 6-13;

encrypting the first session key at the device using a public key(col.3 lines 14-20);

transmitting the encrypted first session key separate from the an encrypted data packet to the server over a link in a first transmission from the mobile device (col.3 lines 14-25);

decrypting the encrypted first session key at the server (col.3 lines 21-33);

adding a header to the encrypted payload to form a data packet at the device (col.4 lines 59-68);

transmitting the data packet in a second transmission from the device to a gateway which recreates the encrypted payload and the header, and forwards the encrypted payload and the header to the server (col.3 lines 21-33);

wherein the server utilizes the decrypted first session key, decrypted from the first transmission to decrypt the encrypted payload (col.3 lines 27-31).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key and decrypting the encrypted data packet at the gateway. Kaufman also fails to specifically disclose the wireless capabilities provided for within the instant application including the wireless link and mobile device.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireless networks and mobile devices that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second session key to provide for heightened security for the information provided in the data packet as well as

the wireless links and devices as described in Droge to provide for increased network flexibility.

As per **claim 11**, the combined method of Kaufman and Droge teaches wherein the decrypting the encrypted first session key at the server further comprises: decrypting the encrypted first session key at the server using a private key associated with the public key (Kaufman col.3 lines 27-31).

As per **claim 16**, the combined method of Kaufman and Droge teaches generating the first session key at the device based on a random number (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 17,** the combined method of Kaufman and Droge teaches wherein the encrypting the payload at the device using the first session key further comprises encrypting the payload at the device using the first session key, wherein the first session key employs an encryption algorithm selected from a group of the encryption algorithms consisting of DESX and DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 20**, the combined method of Kaufman and Droge teaches implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 26**, the combined method of Kaufman and Droge teaches utilizing a random number ot generate the first key (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 27**, the combined device of Kaufman and Droge teaches a memory coupled to the encryption engine, wherein the memory stores the second key, and wherein the encryption engine accesses the second key from the memory (col.3 lines 6-20).

As per **claim 29**, Kaufman teaches a computer readable storage medium, comprising program instruction for performing a method comprising:

encrypting a payload according to a first key (col.3 lines 6-13);

adding a header to the encrypted payload to form a data packet (col.4 lines 59-68);

encrypting the first key according to a second key (col.3 lines 14-20);

transmitting the encrypted first key separate from the encrypted data packet to a server in a first transmission from a mobile device (col.3 lines 14-20); and

transmitting the data packet over the link to a gateway in a second transmission from the device (col.3 lines 21-33), wherein the gateway recreates the encrypted payload and the header (col.3 lines 21-33), and forwards the encrypted payload and the header to the server which decrypts the encrypted first key received in the first transmission (Kaufman col.3 lines 27-31) and decrypts the encrypted payload using the decrypted first key (Kaufman col.3 lines 27-31).

Kaufman fails to specifically disclose encrypting the data packet according to a second session key configured for secured communications over a wireless link and decrypting the encrypted data packet. Kaufman also fails to provide for the use of wireless links and devices within his system.

Droge describes a system and method for highly secure data communications which involves encrypting payload data a first time, packetizing the data, encrypting the data packet a second time and transmitting the data twice-encrypted (see Droge Abstract; paragraphs 12-13, 36-37, 40-42, and 50; figures 5 and 6). Droge also discloses the use of both wireless networks and mobile devices that may be used within his heightened security system (Droge paragraphs 36 and 40).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Kaufman the encryption and decryption of the data packet as described in Droge using Kaufman's already disclosed second key to provide for heightened security for the information provided in the data packet as well as the wireless links and devices as described in Droge to provide for increased network flexibility.

As per **claim 30**, the combined method of Kaufman and Droge teaches wherein the first key comprises a symmetric key (Kaufman col.3 lines 6-13).

As per **claim 31**, the combined method of Kaufman and Droge teaches receiving the data packet at the gateway (Kaufman col.3 lines 27-31);

decrypting the data packet at the gateway according to the third key (Droge paragraph 13);

forwarding the encrypted payload to the server (Droge paragraph 13);

receiving the encrypted first key at the server (Kaufman col.3 lines 27-31);

decrypting the encrypted first key using a fourth key (Kaufman col.3 lines 27-31); and

decrypting the payload according to the decrypted first key (Kaufman col.3 lines 27-31).

As per **claim 32**, the combined method of Kaufman and Droge teaches wherein the first session key comprises a symmetric session key (Kaufman col.3 lines 6-13).

As per claim 33, the combined method of Kaufman and Droge teaches implementing an encryption algorithm selected from a group of encryption algorithms consisting of DESX and DES (Kaufman col.5 lines 24-29, col.6 lines 62-68).

As per **claim 35**, the combined method of Kaufman and Droge teaches wherein the symmetric session key is generated based on a random number (Kaufman col.5 lines 24-29, col.6 lines 62-68).

Claims 8, 15, 25, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Droge and Kaufman as disclosed above

and further in view of United States Patent Application Publication No. 2007/0259655 A1 to Minborg et al.

As per **claim 8,** the combined method of Kaufman and Droge teaches wherein the payload comprises location information (Kaufman col.4 lines 59-68).

The combination of Kaufman and Droge fails to specifically disclose wherein the payload comprises GPS location information obtained by the device regarding a geographical location of the device.

Minborg describes the ability of mobile communication devices to identify their physical location using GPS (par 10) including the ability of mobile communication devices to transmit this GPS location information, in the form of code containing GPS coordinates, a postal code, or some other suitable code generated automatically by the device, within their payloads to devices to which they are communicating (par 60).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the combined system of Kaufman and Droge the GPS location and transmission capabilities as described in Minborg to provide for a system wherein mobile devices may communicate their location to one another securely and efficiently.

As per **claim 15**, the combined method of Kaufman and Droge teaches wherein the payload includes location information (Kaufman col.4 lines 59-68).

The combination of Kaufman and Droge fails to specifically disclose wherein the payload includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device.

Minborg describes the ability of mobile communication devices to identify their physical location using GPS (par 10) including the ability of mobile communication devices to transmit this GPS location information, in the form of code containing GPS coordinates, a postal code, or some other suitable code generated automatically by the device, within their payloads to devices to which they are communicating (par 60).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the combined system of Kaufman and Droge the GPS location and transmission capabilities as described in Minborg to provide for a system wherein mobile devices may communicate their location to one another securely and efficiently.

As per **claim 25**, the combined method of Kaufman and Droge teaches wherein the payload includes location information (Kaufman col.4 lines 59-68).

The combination of Kaufman and Droge fails to specifically disclose wherein the payload includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device.

Minborg describes the ability of mobile communication devices to identify their physical location using GPS (par 10) including the ability of mobile communication devices to transmit this GPS location information, in the form of code containing GPS

coordinates, a postal code, or some other suitable code generated automatically by the device, within their payloads to devices to which they are communicating (par 60).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the combined system of Kaufman and Droge the GPS location and transmission capabilities as described in Minborg to provide for a system wherein mobile devices may communicate their location to one another securely and efficiently.

As per **claim 34**, the combined method of Kaufman and Droge teaches wherein the payload includes location information (Kaufman col.4 lines 59-68).

The combination of Kaufman and Droge fails to specifically disclose wherein the payload includes GPS location information obtained by the mobile device and associated with a geographical location of the mobile device.

Minborg describes the ability of mobile communication devices to identify their physical location using GPS (par 10) including the ability of mobile communication devices to transmit this GPS location information, in the form of code containing GPS coordinates, a postal code, or some other suitable code generated automatically by the device, within their payloads to devices to which they are communicating (par 60).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within the combined system of Kaufman and Droge the GPS location and transmission capabilities as described in Minborg to provide for a

system wherein mobile devices may communicate their location to one another securely and efficiently.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437